International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:7, No:1, 2013

Trust and Reliability for Public Sector Data

Klaus Stranacher, Vesna Krnjic, and Thomas Zefferer

***Abstract*—**The public sector holds large amounts of data of various areas such as social affairs, economy, or tourism. Various initiatives such as Open Government Data or the EU Directive on public sector information aim to make these data available for public and private service providers. Requirements for the provision of public sector data are defined by legal and organizational frameworks. Surprisingly, the defined requirements hardly cover security aspects such as integrity or authenticity.

In this paper we discuss the importance of these missing requirements and present a concept to assure the integrity and authenticity of provided data based on electronic signatures. We show that our concept is perfectly suitable for the provisioning of unaltered data. We also show that our concept can also be extended to data that needs to be anonymized before provisioning by incorporating redactable signatures. Our proposed concept enhances trust and reliability of provided public sector data.

***Keywords*—** Trusted Public Sector Data, Integrity, Authenticity, Reliability, Redactable Signatures.

I. Introduction

DURING the past few years, various developments in the IT sector have been significantly influenced by the so called "open movement". For instance, Open Source has become a well-known term that describes the philosophy of making source code publicly available to everybody. Also related concepts such as Open Access or Open Content have continuously gained popularity during the past years. Recently, especially the concept of *Open Data* has attracted attention. The general idea behind Open Data is that data should be freely available for everyone to be used and republished. Focus is thereby mainly put on non-textual data such as maps, genomes, or statistics, to name but a few.

Considering the different categories of data that are potentially affected by Open Data, it is hardly surprising that the public sector represents one of the most relevant data sources. The importance of governments and related public sector institutions is emphasized by different initiatives that deal with the provision of open data by the public sector.

An example is the *Open Government Data* (OGD) initiative. OGD can be seen as a subset of Open Data and pertains to data being under control of governmental institutions. Numerous OGD initiatives have been started recently in various countries and allow the provision of services based on data supplied by governmental organizations. For instance, in Vienna, Austria, more than 40 applications[1] that make use of OGD provided by the city government are already available for citizens ranging from various mobile smartphone apps to complex applications for desktop computers.

In addition, the public sector collects, creates, reproduces, and disseminates comprehensive sets of data in many areas such as social affairs, economy, weather, tourism, business, and education. Based on these data, new digital-content based products and services can be developed. The European Union considers this as a key factor for accessing and acquiring knowledge as well as rapid job creation, especially in small emerging companies. Therefore, the Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information [10] (hereinafter referred to as *PSI Directive*) has been published. The directive defines a common legal framework for the provision of public data and the re-use of information sources enabling the *"harmonisation of the rules and practices in the Member States relating to the exploitation of public sector information"* [10].

In general, the term *public sector data* denotes all kinds of electronic data being produced, collected, provided, or simply processed by the public sector. In this paper we focus on public sector data used in the context of the OGD initiative and the PSI Directive. However, the methods proposed in this paper are not limited to these use cases.

Given the growing relevance and popularity of using public sector data in the public domain, security issues have been astonishingly rarely discussed so far. In literature, several requirements have been defined for OGD solutions [9]. However, security aspects such as data integrity or authenticity are hardly ever mentioned. Also the PSI Directive defines a set of basic requirements for solutions dealing with public sector information but does not clearly define data integrity or authenticity as a requirement.

Security in general and selected security aspects such as data integrity and authenticity in particular are without doubt important factors that should also be considered by public sector data based solutions. The use of forged data might for instance lead to resource claims. In such cases, the supplier of data should be able to proof that originally provided data has been altered. Current solutions based on public sector data usually do not support this feature.

In this paper, we propose a method that makes use of electronic-signature concepts in order to assure the integrity and authenticity of provided public sector data and information. Electronic signatures rely on public-key cryptography and basically represent the electronic equivalent

Klaus Stranacher is with the E-Government Innovation Center, Inffeldgasse 16a, 8010 Graz, Austria (e-mail: klaus.stranacher@egiz.gv.at).

Vesna Krnjic is with the E-Government Innovation Center, Inffeldgasse 16a, 8010 Graz, Austria (e-mail: vesna.krnjic@egiz.gv.at).

Thomas Zefferer is with the Secure Information Technology Center - Austria, Inffeldgasse 16a, 8010 Graz, Austria (e-mail: thomas.zefferer@a-sit.at).

[1] See http://www.data.gv.at/

to hand-written signatures. By applying a cryptographic method incorporating a private key to a set of data, the data is unambiguously linked to (i.e. signed by) the holder of the private key. The electronic signature can be verified using the corresponding public key. The verification process can only succeed, if the correct public key is used, and if the signed data is unaltered. Each modification of the signed data immediately breaks the electronic signature. This way, illegitimate alterations of signed data can be detected easily.

While the proposed solution is able to assure the integrity and authenticity of open public sector data, the application of electronic signatures also raises new challenges. In order to meet privacy requirements, data provided for public use needs to be redacted[2], i.e. altered. Of course, the modification of data would break any electronic signature on these data. To overcome this issue, we extend our approach by replacing the concept of electronic signatures by redactable signatures. Redactable signatures are a special kind of electronic signatures that allow for a (limited) modification of signed data without breaking the applied signature. We use redactable signatures to assure the integrity and authenticity of redacted data. This way, the proposed concepts enhance the overall security of solutions relying on public sector data.

The remainder of this paper is structured as follows. In Section II we discuss common requirements of public sector data and argue the need for additional requirements that cover data integrity and authenticity. We discuss electronic signature concepts that will be employed to meet these additional security requirements in Section III. Based on this theoretical foundation, we introduce our concepts to assure integrity and authenticity of public sector data using electronic and redactable signatures in Section IV. Final conclusions are drawn in Section V.

II. Common Requirements for Public Sector Data

OGD and PSI are main areas regarding the publishing and provisioning of public sector data. There are already a number of well-defined requirements for OGD as well as for the re-use of public sector information. In 2007, the Open Government Working Group [9] published a set of fundamental principles for Open Government Data. Also the PSI Directive establishes a minimum set of rules governing the re-use of existing documents[3] held by public sector bodies of the EU Member States.

In general, provision of government data in public sector should fulfil a set of requirements in order to assure an appropriate level of quality. In this context, the following aspects should be considered:

1) *Completeness*: OGD principles specify that all government data that are not subject to privacy or security restrictions should be made publicly available. The PSI Directive does not mention completeness of data explicitly. Provision of all appropriate documents held by the public sector is one of the goals of PSI. With regard to privacy, the PSI Directive states that: *"The Directive should be implemented and applied in full compliance with the principles relating to the protection of personal data in accordance with Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and of the free movement of such data."* [10].

2) *Primary Source*: OGD principles state that: *"Data should be published and collected at the source with the finest possible level of granularity, not in aggregate or modified forms."* [9]. The PSI Directive does not explicit provide any guidance for a primary source of data. It can be assumed that data provided by a public sector body fulfil this requirement.

3) *Timely Available*: OGD should be made available as fast as possible to the public. The benefit for the public can be enhanced through real-time update of time-dependent data. For PSI, there are no explicit rules for regulating the timely provision of documents. In the PSI Directive (12) is recorded that *"public sector bodies should make the documents available in a time-frame that allows their full economical potential to be exploited."* [10].

4) *Accessibility*: Public data must be made available barrier-free to widest range of users. The need for physical access to data (e.g. the attendance of special premises) should be avoided as well as the use of special electronic technologies. PSI data are not constricted to electronic data so the access to these data is not only through the Internet. Article 3 of the PSI Directive states that *"Where possible, documents shall be made available through electronic means."* [10].

5) *Machine Processible*: OGD should be stored in widely used file formats so that they could be automatically processed in order to ensure an easy integration in software applications. If data were normalized a sufficient documentation should be provided about the used file format. Likewise, the raw data should be available, which can be downloaded automatically. Article 5 of the PSI Directive states that *"Public sector bodies shall make their documents available [...] through electronic means where possible and appropriate."* [10].

6) *Data Access*: An anonymous access to the OGD should be possible for all users at any time. The access to the data should not be restricted to certain organizations or groups of people. Furthermore, users should not be forced to use certain software applications. In general PSI documents are not available for free. Therefore public sector documents usually need request for reuse (e.g. licence is needed).

7) *Non-Proprietary*: OGD specify the use of open standards to ensure that reading and processing of provided data does not require specific software. In most cases, it is necessary to provide data in different formats. PSI Directive states that *"Public sector bodies shall make their documents available in any pre-existing format or language [...]."* [10].

8) *License*: Open Government Data are license-free and not subject to any copyright. While in contrast the re-use of PSI imposes no strict guidelines. The Directive (Article 8)

[2] Redact means to make (portions of) a text unrecognizable (anonymization) or to substitute it with another text.

[3] The PSI Directive defines documents as *"any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audiovisual recording)"* [10]. For our following considerations we refer on electronically available data, which come under the Directive.

proposes that: *"Public sector bodies may allow for re-use of documents without conditions or may impose conditions, where appropriate through a licence, dealing with relevant issues."* and *"In some cases the re-use of documents will take place without a licence being agreed. In other cases a licence will be issued imposing conditions on the re-use by the licensee dealing with issues such as liability, the proper use of documents, guaranteeing non-alteration and the acknowledgement of source."* [10]. In addition, the Directive states that charges *"shall not exceed the cost of collection, production, reproduction and dissemination […]"* [10].

Table I summarizes the different requirements of public sector data and compares their impact on OGD and PSI.

TABLE I
OVERVIEW OGD AND PSI DIRECTIVE REQUIREMENTS

Requirement	Open Government Data	PSI Directive
Completeness	Data must be complete and privacy regulations must be taken into account.	Privacy regulations must be taken into account.
Primary Source	Data must originate from the primary source.	Not explicit mentioned, but public sector body should count as primary source.
Timely available	Data should be published as fast as possible.	Data should be provided in an appropriate time-frame.
Accessibility	Data should be published barrier-free and the need for physical access avoided.	Data is not restricted to electronic data, but shall be made available electronically.
Machine processible	Data should be in automatically proccesible formats.	Data should be provided through electronic means (where possible and appropriate)
Data Access	An anonymous access for anybody at any time should be provided.	Data is usually not publicly available and a request for reuse is needed.
Non-Proprietary	Data formats should base upon open standards to ensure the long-term readability.	Data should be available in any pre-existing format.
License	Data must be license-free and not subject to any copyright	No strict guidelines defined. Data may be provided under designated and non-discriminatory conditions

The focus of the above-mentioned principles of OGD and the re-use of PSI targets on completeness, timeliness, and accessibility of data. Security aspects have not been included, except the usage restriction of personal data. However, depending on the use case scenario we strongly recommend compliance with appropriate security requirements, especially for providing and publishing public sector data. We consider the previously defined requirements for public sector data (for certain scenarios) as incomplete and hence insufficient. Therefore, we extend the general principles by the following two requirements in order to appropriately consider security aspects:

1) *Authenticity and Integrity*: The authenticity and integrity of public sector data should be ensured by the use of appropriate cryptographic procedures. This shall establish that recipients of these data can check unauthorized modification (integrity) and beyond everyone can identify the provider of the data unambiguously (authenticity).

2) *Authenticity and Integrity for Redacted Government Data*: As defined in previous section of general requirements for public sector data, personal data must not be published as Open Government Data or be provided as public sector information because they underlie data privacy constraints. Often, the general information linked to these personal data can be of interest for the public and still be useful. Therefore, such data should be redacted in an appropriate way and thereafter be published without any privacy violation. This requirement must not be in conflict with the demand for authenticity and integrity. In any case, the authenticity and integrity of the redacted data must be ensured.

The discussed requirements extension for public sector data is a serious challenge for public sector bodies. A consideration of these extensions will necessarily include the integration of well-established and upcoming electronic signature concepts.

Therefore, the following Section III will present and discuss the cryptographic concepts that allow consideration of the defined extended requirements. Concrete concepts to implement appropriate procedures to take account of the extended requirements are finally discussed in Section IV.

III. CONCEPTS FOR ELECTRONIC SIGNATURES

In general, electronic signatures are used to provide a proof of genuineness for electronic data. Hence, electronic signatures represent the counterpart to hand-written signatures on paper based documents. Electronic signatures basically assure authenticity, data integrity, and non-repudiation of origin. The receiver of a signed document is able to uniquely identify the creator of the signature[4] (authenticity) and is able to verify that the signed data has not been modified (integrity). At the same time, the creator of an electronic signature cannot deny to have signed the data (non-repudiation). Especially the validation of data integrity becomes important for security-critical applications. For instance, in case of an electronically signed contract the content of the contract cannot be unilaterally modified without invalidating the electronic signature. We use the properties of electronic signatures to ensure both integrity and authenticity for public sector data. In the European Union, electronic signatures are widely used in transactional e-government processes and rely on a common legal basis formed by the EU Signature Directive [11] and their national implementations.

During the past decades, different forms of electronic signatures with different properties and characteristics have been developed. The security-enhancing concepts proposed in this paper basically rely on conventional electronic signatures and redactable signatures. We discuss relevant properties of these cryptographic methods in the following subsections.

[4] The creator of a signature is also called signatory.

A. Conventional Electronic Signatures

The technical basis for electronic signatures is public key cryptography. The creator of an electronic signature holds a private and a public key. The creator has sole control over the private key, which is used to create the signature[5]. Fig. 1 (a) illustrates the basic principle of a typical signature-creation process. In a first step, the signed data is mapped to a hash value of a fixed length using a so called hash function[6]. This hash value is then signed using the signatory's private key. The corresponding public key is published[7] and the receiver of the signed data is able to verify the validity of the signature by means of this public key.

Usually, the receiver of signed data wants to verify the validity of the obtained electronic signature. Therefore, the receiver executes a signature verification process as shown in Fig. 1 (b). As a first step, a hash value comparison is carried out. To do so, the verifier computes a hash value over the received signed data. The resulting hash value is then compared to the original hash value that can be extracted out of the obtained electronic signature. If these two hash values match, the data has not been altered[8]. If there is a difference between the two hash values, the data has obviously been modified after the signing process. In a second step (if the hash values are equal) the verifier checks if the public key matches the private key by applying the public key on the obtained signature value. If there is a match[9], the signature is called valid, otherwise invalid.

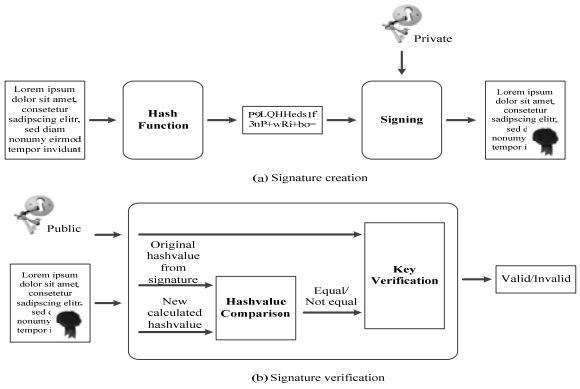

Fig. 1 Basic principle of electronic signatures

A fundamental property of conventional electronic signatures is that each modification of signed data leads to an invalidity of the signature. During the signature verification process, the hash value of the modified data is compared to the hash value of the original data. As the hash value of the modified data differs from the original hash value, the verification process results in an invalid signature. This way, the receiver of the signed data is able to detect modifications during the signature verification process.

For conventional electronic signatures a variety of different signature formats have been developed. For instance, XMLDSIG [12] and XAdES [13] are well established XML based signature formats. Similarly, Adobe PDF signatures [14] or PAdES [15] are commonly used signature formats for the signing of PDF documents.

B. Redactable Signatures

There exist use cases, in which a modification of signed data should be possible without leading to an invalidity of the signature. Such a use case is for instance the anonymization of data including personal and private data, which must not be published for legal and privacy reasons. *Redactable signatures* are a cryptographic concept, which allows a subsequent modification of signed data without invalidating the original signature. The person who is able to perform such modification is called the *redactor*.

The concept of redactable signatures is discussed in detail in [1]. The authors of this article define different properties of redactable signatures. These properties can be used to classify the different existing schemes for redactable signatures. The following properties exist:

1) *Property P1 – Designated Redactor*: This property defines if signed data can be modified by everybody or exclusively by a designated redactor, which is explicitly defined by the signatory.

2) *Property P2 – Replacement of Blocks*: This property defines if a redactor is able to delete (blacken out) text blocks only, or if the redactor is also able to replace it with other text blocks.

3) *Property P3 – Designated Parts*: A signatory is able to determine if a redactor is able to redact all text blocks or only designated blocks.

4) *Property P4 – Recognizable Modification*: This property defines if a modification of a redactor is recognizable afterwards.

5) *Property P5 – Controlled Replacement*: This property specifies if a signatory is able to control which text blocks can be used for the replacement (e.g. a certain text block can be defined to be replaceable by the text blocks "Yes" or "No" only).

By combining these properties, several different redactable signature schemes can be derived. The following Table I gives an overview of different redactable signature schemes and compares their properties.

[5] An important characteristic is that the private key cannot be determined out of the public key and is infeasible to guess.

[6] A hash function is a one-way function, which creates a fixed length checksum (hash value) out of arbitrary length data. Fundamental properties of hash functions are that it is neither possible to determine the original data out of a given hash value (pre-image resistance), nor to find another data, which maps to the same hash value (second-pre-image and collision resistance). The main reason for applying a hash function is that, in general, the data to be signed is quite large and signing large data is very inefficient and time consuming for practical applications.

[7] The public key is usually published via a trusted third party using an electronic certificate. This certificate holds the public key of the signatory and binds the signatory's identity to this key.

[8] This means the integrity of the data has been successfully checked.

[9] This means the signatory is the very person he or she claims to be.

TABLE I
REDACTABLE SIGNATURE SCHEMES AND THEIR PROPERTIES [1]

Signature Schema	P1	P2	P3	P4	P5
Content Extraction Signatures [2]	No	No	Partly	Yes	No
Sanitizable Signatures [3]	Yes	No	Yes	No	No
Homomorphic Signature Schemes [4]	No	No	No	Yes	No
Extended Sanitizable Signatures [5]	Yes	Yes	Yes	Yes	Yes
Extended Sanitizable Signature Schemes [6]	Yes	Yes	Yes	Yes	Yes
Generalizations and Extensions of Redactable Signatures [7]	No	Yes	Partly	Yes	Yes
Efficient signature schemes [8]	No	No	Yes	Yes	No

Independent from the respective scheme, the basic principle of all redactable signatures is the same. All schemes base on retention of the hash value of the original and unmodified data. For conventional electronic signatures, a different hash value indicates a modification of the signed data and leads to an invalid signature. However, if the original hash value is retained and used during the signature verification (instead of the new calculated hash value) the original signature can be validated successfully.

Fig. 2 shows the basic principle of redactable signatures by means of a simple example. It explains how a text is signed, afterwards redacted, and finally verified successfully. For the signature creation, a message m is divided into five text blocks m_1 to m_5. For each of these blocks, a hash function H is applied and the hash values h_1 to h_5 are computed. Based on these hash values, a total hash value H_{TOTAL} is calculated. This total hash value is then signed to create the signature S.

According to the example shown in Fig. 2, the text block *"redacted"* is then blacked out (message block m_{4*}). This leads to a hash value h_4, which differs from the original hash value[10] and would result in an invalid signature. To avoid this invalidity, the original hash value is used during the signature verification process[11].

Of course, this approach requires the receiver of the signature, who usually performs the signature verification, to receive the hash value h_4 in addition to the signature. Hence, the receiver, who only knows the redacted message, is able to verify the original signature without knowing the text block m_4. Due to the one-way functionality of the hash function, the receiver is not able to determine the redacted text block. By using conventional hash functions in association with a small number of potential text blocks (e.g. if only first names are possible for the redacted text block), there is a risk that the redacted text can be reconstructed by just trying all possible combinations. Thus, for real applications randomized hash functions are used. These hash functions are using an additional random value to calculate the hash value, which hinders a simple guessing of the text block.

Conventional electronic signatures are able to ensure authenticity and integrity for public sector data, whereas redactable signatures work well to fulfil the requirement for authentic and integrity-protected redacted public sector data as defined in Section II. In the following section we introduce our concept for a *trusted public sector data*, which bases on conventional and redactable signatures.

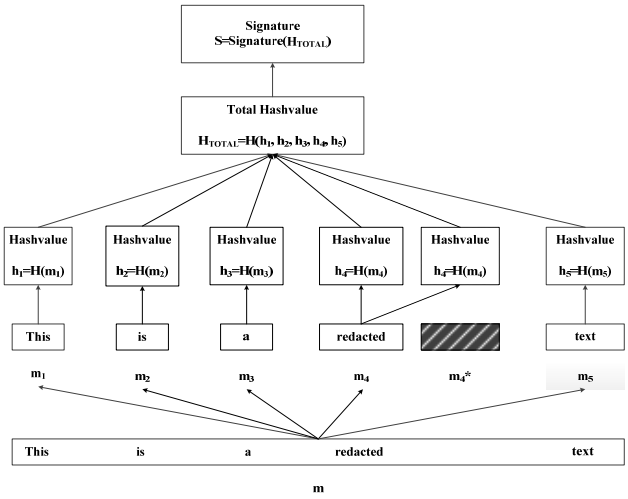

Fig. 2 Basic principle of redactable signatures

IV. TRUSTED PUBLIC SECTOR DATA

The objective of the presented concept is to ensure authenticity and integrity for public sector data including the possibility to anonymize or redact (parts of) these data. To fulfil these requirements, the proposed concept integrates conventional and redactable signature schemes as outline in Section III. In the following we discuss details of this concept and show how providers as well as recipients of public sector data benefit from this approach.

By using electronic signatures for public sector data, two general use cases can be distinguished. Depending on the use case, our concept makes use of different schemes for electronic signatures. In the following, the two general use cases covered by our concept are presented in detail.

A. Use Case 1: Ensuring Authenticity and Integrity for Public Sector Data

In this scenario we show how a provider of public sector data is able to provide authentic and integrity-protected data. Providing such secured data has following advantages:

1) *Integrity of the Data*: By ensuring the integrity of data, subsequent modifications of the data can be detected. Both, the data provider and the recipient of the data benefit from this feature. The recipient is able to trust the validity and correctness of the provided data. For the provider this feature guarantees that recipients cannot claim to have received incorrect data.

2) *Authenticity of the Data Provider*: The recipient of the public sector data is able to reliably determine the identity of the data provider. This leverages the trust in the reliability and trustworthiness of the provided data.

[10] $H(m_4)$ is unequal to $H(m_{4*})$.
[11] I.e. $H(m_4)$ is used for calculating H_{TOTAL} instead of $H(m_{4*})$.

The means of choice for implementing authentic and integrity-protected public sector data are conventional signature schemes. Fig. 3 illustrates the basic approach. The original public sector data source is located in the domain of the public sector data provider. These data is signed with the private signature key of the provider. Depending on the data format, different signature formats are possible. For instance, XML-based or PDF-based signatures are promising candidates, but basically each suitable signature format is applicable. Afterwards, the signed data is provided or published through appropriate communication channels as trusted public sector data[12].

To verify the authenticity and integrity of the data, the recipient can verify the electronic signature. In case of a valid signature the recipient has evidence that the data has not been altered or modified. Additionally, the recipient is assured that the data has been provided by the respective provider.

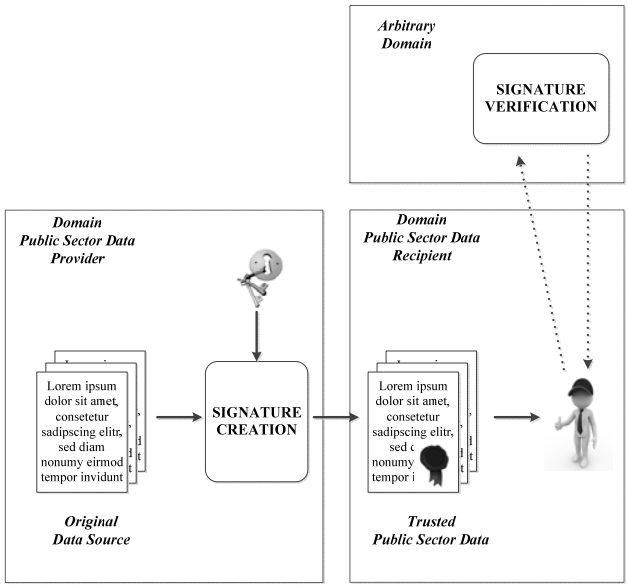

Fig. 3 Use case 1 – Ensuring authenticity and integrity for public sector data

B. Use Case 2: Authenticity and Integrity for Redacted Public Sector Data

This use case covers all applications, in which the original data set contains personal and private data. Usually, such data is prohibited for processing due to legal and privacy reasons. However, there exist applications where general data being linked to the private data is suitable to be reused. Hence, there is a need to anonymize or to redact the original personalized or private data.

For use case 1, a concept using conventional signatures to achieve authenticity and integrity has been proposed. This approach is not practical for the second use case. The anonymization process leads to a modification of the signed data and therefore to an invalid signature. In order to achieve trusted public sector data, the anonymized or redacted data must be signed again. For some applications, this is however no practical or feasible approach. For instance, the original signatory could not be available or a renewed signature creation could not be possible for other reasons. At this point redactable signatures produce a relief.

Fig. 4 shows the basic principle of trusted public sector data based on redactable signatures. The provider of the public sector data uses its private key to create a redactable signature. The redactor anonymizes or redacts the data and updates the redactable signature (i.e. adding the appropriate original hash values of the redacted blocks). For this purpose, the redactor must use his or her private key, if the provider has defined that only designated redactors are able to modify the signed data. After this, the redactable signature and the modified data are made available for the recipient. The recipient is able to verify the original signature without gaining access to the anonymized or redacted data. In case of a positive signature verification result, the recipient can again trust on the authenticity and integrity of the obtained data.

Depending on the concrete use case, different redactable signature schemes may be used. Depending on the properties of the chosen signature scheme, the provider is able to define designated redactors (property P1) or may define which parts of the data can be anonymized or redacted (property P2).

V. Conclusion

In this paper, we have proposed two concepts to assure the integrity and authenticity of public sector data being provided for re-use. Our first concept makes use of conventional electronic signatures to guarantee integrity and authenticity of arbitrary provided data. As conventional electronic signatures cannot be successfully applied if the signed data needs to be modified after the signature-creation process, this concept is not suitable for the provision of data that needs to be redacted. For these scenarios, we have proposed a second concept that relies on redactable signature schemes. These signature schemes allow for a successful signature-verification process, even if signed data needs to be modified.

By applying the proposed concepts, providers of public sector data can easily assure the integrity and authenticity of data intended for re-use by external parties. This leverages an appropriate level of security for solutions based on provided public sector data and is advantageous for both providers and recipients of data. Recipients can be sure that obtained data is genuine, unmodified, and stems from the expected source. At the same time, data providers benefit from the application of electronic signatures, as recipients cannot claim to have obtained incorrect data.

The different signature schemes, which the proposed concepts rely on, are already well established and frequently used in various security-sensitive fields of application. Software modules that facilitate the creation and verification of electronic signatures are publicly available and already frequently used in e-government and related fields of application. The implementation of a prototype application

[12] E.g. in the context of Open Government Data, these data may be published through publicly accessible interfaces. For data based on the PSI Directive the provider may give the recipient an appropriate access to the data.

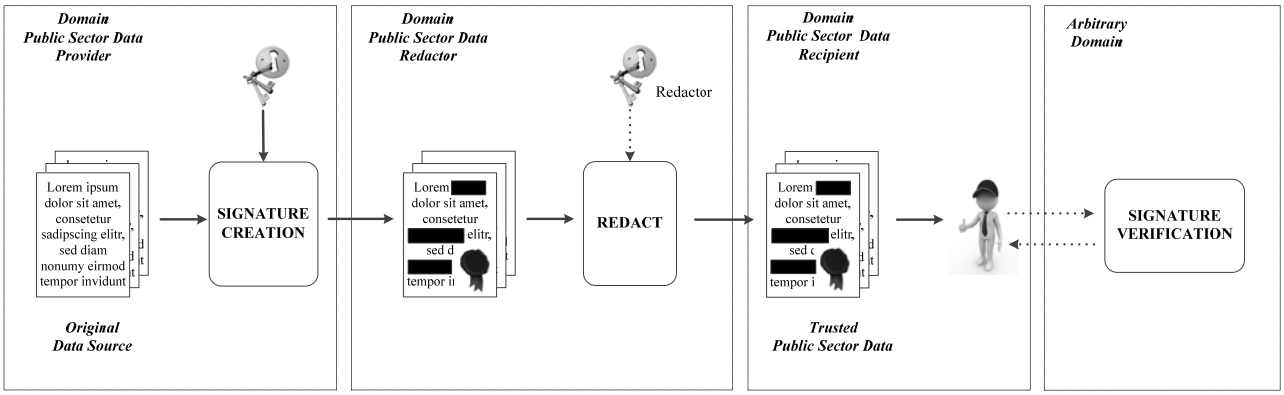

Fig. 4 Use case 2 – Authenticity and integrity for redacted public sector data

that relies on existing software solutions and incorporates the concepts proposed in this paper will demonstrate the practical applicability of our approach and is regarded as future work.

REFERENCES

[1] D.Slamanig und S.Rass, "Redigierbare Signaturen: Theorie und Praxis" in: Datenschutz und Datensicherheit, Bd. 35, Nr. 11, S. 757-762.
[2] R. Steinfeld, L. Bull und Y. Zheng: Content Extraction Signatures. ICISC, LNCS 2288, S. 285-304. Springer, 2001.
[3] G. Ateniese, D. H. Chou, B. de Medeiros und G. Tsudik. Sanitizable Signatures. ESORICS, LNCS 3679, S. 159-177. Springer, 2005.
[4] R. Johnson, D. Molnar, D. X. Song und D. Wagner. Homomorphic Signature Schemes. CTRSA, LNCS 2271, S. 244-262. Springer, 2002.
[5] M. Klonowski und A. Lauks. Extended Sanitizable Signatures. ICISC, LNCS 4296, S. 343-355. Springer, 2006.
[6] S. Canard und A. Jambert. On Extended Sanitizable Signature Schemes. CT-RSA, LNCS 5985, S. 179-194. Springer, 2010.
[7] D. Slamanig und S. Rass. Generalizations and Extensions of Redactable Signatures with Applications to Electronic Healthcare. CMS, LNCS 6109, S. 201-213. Springer, 2010.
[8] S. Haber, Y. Hatano, et al.: Efficient signature schemes supporting redaction, pseudonymization, and data identification. ASIACCS, S. 353-362. ACM, 2008.
[9] Open Government Working Group, 8 Principles of Open Government Data, http://www.opengovdata.org/home/8principles, 2007.
[10] The European Parliament and the Council of the European Union: Directive 2003/98/EC of the European Parliament and the Council of 17 November 2003 on the re-use of public sector information, Official Journal of the European Union L 345/90, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003L0098:EN:NOT, 2003.
[11] The European Parliament and the Council of the European Union: Directive 1999/93/EC of the European Parliament and the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal of the European Union L 13/12, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31999L0093&model=guichett&lg=en, 2000.
[12] W3C Recommendation: XML-Signature Syntax and Processing (Second Edition), http://www.w3.org/TR/xmldsig-core/, 2008.
[13] ETSI TS 101 903, Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES), V1.4.2, 2010
[14] Adobe Corporation, Document management — Portable document format — Part 1: PDF 1.7, First Edition, 2008.
[15] ETSI TS 102 778-1, Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES, V1.1.1, 2009.

Klaus Stranacher finished his MSc with distinction in Telematics at the University of Technology in the year 2006. Since 2005 he is working at the E-Government Innovation Center (EGIZ) in Graz. His main activities are in the area of E-Government and IT security especially on electronic identities, electronic documents and interoperability. During his activities he participates in several European research projects. He was involved the European electronic identity large scale pilot STORK (Secure IdentTity acrOss boRders linKed) and he is the leader of work package 2 (eDocuments) in the European large scale pilot SPOCS (Simple Procedures Online for Crossborder Services) under the ICT-PSP (Policy Support Programme), co-founded by EU. Additional he is working on his PhD thesis on interoperability of electronic documents, which is also his main research interest.

Vesna Krnjic finished her BSc with distinction in Informatics at the University of Technology Graz in the year 2010. Since 2010 she is working at the Institute for Applied Information Processing and Communications at the University of Technology Graz. Her main activities are in the area of E-Government and IT security with focus on usability and testing. Additionally she is working on her master thesis, which is about visual programming languages on smartphones, especially developed for children and teenagers.

Thomas Zefferer finished his MSc with distinction in Telematics at the University of Technology in the year 2007. Since 2007 he is working at the Institute for Applied Information Processing and Communications at the University of Technology Graz. Her main activities are in the area of E-Government and IT security. In the last years he was involved in many projects and activities of the E-Government Innovation Center (EGIZ) and the Secure Information Technology Center – Austria (A-SIT). His research focus lies on smartphone security and mobile E-Government processes, which is also the subject of his PhD thesis.